UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/788,417	03/01/2004	Yoko Kumagai	64235-017	4957

7590 10/27/2008

MCDERMOTT, WILL & EMERY
600 13th Street, N.W.
Washington, DC 20005-3096

EXAMINER	
TABOR, AMARE F	
ART UNIT	PAPER NUMBER
2439	
MAIL DATE	DELIVERY MODE
10/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/788,417	KUMAGAI ET AL.	
	Examiner	Art Unit	
	AMARE TABOR	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/28/2008 has been entered.

2. Claims 1 and 8 are amended.

3. **Claims 1-14** are pending.

Response to Arguments

4. Applicant's arguments with respect to the pending claims have been considered but are moot in view of the new ground(s) of rejection.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided

the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. **Claims 1 and 8** are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of Fujishiro et al. (US 7,080,251 B2 - **"Fujishiro"**) in view of Van Oorschot et al. (US 6,134,550 - **"Van Oorschot"**).

Claim 1 of **Fujishiro** reads as follows	**Claim 1** of the **instant application** reads as follows
A certificate validity authentication method for a public key certificate wherein validity of the public key certificate is authenticated by a computer, wherein, the computer executes:	A method for validating a public key certificate by a computer in a public key infrastructure composed of a plurality of certificate authorities including an end entity certificate issuing authority, wherein:
a path search step of searching a path between any one of a plurality of certification authorities as a start point (a start certification authority) and at least one terminal certification authority which issues the public key certificate to terminals;	the end entity certificate issuing authority issues to an end entity a public key certificate used for validating a signature generated by an end entity apparatus operated by the end entity,
a path verification step of verifying the path searched by the path searching step; a path registration step of registering the path verified by the path verification step in a database; and	the method comprises: path registration step of registering in a database a valid path extending from a certificate authority being a start certificate authority to any end entity certificate issuing authority,
a validity authentication step of receiving a request to authenticate the public key certificate and validating the public key certificate issued by the terminal certification authorities by using information on the verified path registered in the database, and wherein	a certificate validation step of receiving a certificate validation request for a public key certificate issued by any end entity certificate issuing authority, judging the validity of the public key certificate of which the certificate validation has been requested using information registered in the database, and outputting a result of the judgment,
the in the path search step, the computer executes:	the path registration step and the certificate validation step are executed by the computer independently of one another,
	the path registration step comprises the following steps executed by the computer:

a first step of setting the start certification authority as an issue origin certification authority;	step 1) searching a path extending from the start certificate authority to the end entity certificate issuing authority which is the end of the path;
a second step of obtaining issue destinations of all the public key certificates issued by a device of the issue origin certification authority;	
a third step, as to each of the issue destinations obtained in the second step, in a case where the issue destination concerned is one of the plurality of certification authorities, setting a path between the issue destination concerned and the issue origin certification authority, and in a case where the issue destination concerned is one of the terminals, setting the issue origin certification authority as the terminal certification authority, and setting a path comprising at least one of the path thus set, between the start certification authority and the terminal certification authority as the searched path; and	step 2) validating the path searched in step 1, and step 3) registering the path which has been validated in step 2 as a valid path in the database, and the certificate validation step comprises the following steps executed by the computer:
a fourth step, if the issue destinations obtained in the second step include one of the plurality of certification authorities, returning to the second step, and wherein in the path verification step, the computer executes: a fifth step of setting the terminal certification authority as the issue destination certification authority; a sixth step of verifying the signature of the public key certificate issued by the issue destination certification authority with another public key certificate issued by the issue origin certification authority located on the searched path; and	step 4) checking whether there is registered in the database a path specified by the request for certificate validation, the path extending from the start certificate authority being the trust anchor of an originator of the request for certificate validation to the end entity certificate issuing authority which has issued the public certificate of which the certificate validation has been requested, and which is the end of the path, step 5) if the checked path is registered in the database as the valid path in step 4, validating a signature of the public key certificate of which the certificate validation is requested, by using the public key certificate issued to the end entity certificate issuing authority being the end of the checked path, and if validation of the signature is successful, judging that the public key certificate of which the certificate validation has been requested is valid and outputting a result of the judgment; **step 6) if the checked path is not registered in the database as the valid path in step 4, searching a path that includes a partial path from the start certificate authority being the trust anchor to the end entity certificate issuing authority which has issued the public key certificate of which certificate validation is requested and which is the end of the path, and**

a seventh step, in a case where the signature has been verified and the issue origin certification authority on the searched path is **not** the start certification authority, setting the issue origin certification authority as a new issue destination certification authority on the searched path and returning to the sixth step, in a case where the signature has been verified and the issue origin certification authority on the searched path is the start certification authority, setting the searched path as a certification path (verified path).	**that extends from the start certificate authority being the trust anchor to the end entity which is an issue destination of the public key certificate of which certificate validation is requested;** step 7) in the searching step in step 6, if the path extending from the start certificate authority being the trust anchor to the end entity being the issue destination of the public key certificate of which certificate validation is requested is detected, validating the path that includes the partial path and extends from the start certificate authority being the trust anchor to the end entity being the issue destination of the public key certificate of which certificate validation is requested; step 8) judging the validity of the public key certificate of which certificate validation is requested based on the validation result in step 7 and outputting a result of the judgment; and step 9) registering the partial path included in the path validated in step 7 into the database as a valid path.
	Claim 8 of the instant application is **a computer program product** of Claim 1

As indicated in the last office action sent, **Fujishiro** discloses steps 6 through 9 [see at least FIGS.10 and 11, for example]; but fails to disclose the highlighted feature [**'performing the steps if the path is not registered'**] of the instant application as shown in the table above. However, on the same field of endeavor, **Van Oorschot** teaches the missing elements of the limitation as [see FIGS.6, 7A and 7B; and for example, col.10, lines 18-58 – *where **Van Oorschot** discloses the chain constructing unit and chain data generator perform table registering and searching for a partial path if no end is reached*]. Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention was made, to modify the system of **Fujishiro** by incorporating the teachings of **Van Oorschot** and arrive at the claimed feature of the instant application. The modification is beneficial to facilitate a rapid validity determination of public certificates [see at least abstract of **Van Oorschot**].

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fujishiro et al. (US 2002/0046340 A1 - "Fujishiro") in view of Van Oorschot et al. (US 6,134,550 - "Van Oorschot")

As per Claim 1, Fujishiro teaches,

A method for validating a public key certificate by a computer in a public key infrastructure composed of a plurality of certificate authorities including an end entity certificate issuing authority, wherein the end entity certificate issuing authority issues to an end entity a public key certificate used for validating a signature generated by an end entity apparatus operated by the end entity, the method comprises: a path registration step of registering in a database a valid path extending from a certificate authority being a start certificate authority to any end entity certificate issuing authority (see *REGISTER PATHS WHOSE VERIFICATIONS HAVE HELD GOOD, IN PATH DB S1004 in FIG.*7; and for example, par.[0021]),

a certificate validation step of receiving a certificate validation request for a public key certificate issued by any end entity certificate issuing authority, judging the validity of the public key certificate of which the certificate validation has been requested using information registered in the database, and outputting a result of the judgment (see *S2002 in FIG.*10; and for example, par.[0020]), the path registration step and the certificate validation step are executed by the computer independently of one another (see *PATH DB 31 and PATH VERIFICATION UNIT 33 in FIG.5*), the path registration step comprises the following steps executed by the computer: step 1) searching a path extending from the start certificate authority to the end entity certificate issuing authority which is the end of the path (see *S2002 in FIG.*10; and for example, par.[0063]);

step 2) validating the path searched in step 1(see *S2008 in FIG.*11; and for example, par.[0064], lines 1-3 and par.[0085]); and step 3) registering the path which has been validated in step 2 as a valid path in the database (see *S1004 in Fig.*7; and for example, par.[0064], lines 3-5 and [0092]), and

the certificate validation step comprises the following steps executed by the computer: step 4) checking whether there is registered in the database a path specified by the request for certification validation, the path extending from the start certificate authority being the trust anchor of an originator of the request for certificate validation to the end entity certificate issuing authority which has issued the public certificate of which the certificate validation has been requested, and which is the end of the path (see *VALIDITY TERM/REVOCATION STATE EXAMINATION UNIT 34 in FIG.5*; and for example, par.[0065]),

step 5) if the checked path is registered in the database as the valid path in step 4, validating a signature of the public key certificate of which the certificate validation is requested, by using the public key certificate issued to the end entity certificate issuing authority being the end of the checked path, and if validation of the signature is successful, judging that the public key certificate of which the certificate validation has been requested is valid (see *VALIDITY TERM/REVOCATION STATE EXAMINATION UNIT 34 in FIG.5*; and for example, par.[0065]) and outputting a result of the judgment (see *COMMUNICATION UNIT 36 in FIG.5*);

step 7) in the searching step in step 6, if the path extending from the start certificate authority being the trust anchor to the end entity being the issue destination of the public key certificate of which certificate validation is requested is detected, validating the path that includes the partial path and extends from the start certificate authority being the trust anchor to the end entity being the issue destination of the public key certificate of which certificate validation is requested (see *VALIDITY AUTHENTICATION UNIT 35 in FIG.5;* and for example, par.[0067]);

step 8) judging the validity of the public key certificate of which certificate validation is requested based on the validation result in step 7 and outputting a result of the judgment (see *COMMUNICATION UNIT 36 in FIG.5 and Step 2008 in FIG.11;* and for example, par.[0109]); and step 9) registering the

partial path included in the path validated in step 7 into the database as a valid path (see for example, par.[0079] to [0085]).

Fujishiro discloses steps 6 through 9 [see FIGS.10 and 11, for example]; but fails to disclose performing the steps if the path is not registered and searching a path that includes a partial path; however, on the same field of endeavor, **Van Oorschot** teaches the missing elements of the limitation [see FIGS.6, 7A and 7B; and for example, col.10, lines 18-58 – *where **Van Oorschot** discloses the chain constructing unit and chain data generator perform table registering and searching for a partial path if no end is reached*]. Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention was made, to modify the system of **Fujishiro** by incorporating the teachings of **Van Oorschot** in order to facilitate a rapid validity determination of public certificates [see at least abstract of **Van Oorschot**].

Claim 8 is a computer program product claim of the method recited in Claim 1. It is rejected for the same rationale applied to the rejection of the method of Claim 1.

As per Claim 2, Fujishiro-Van Oorschot combination teaches,

Step 10) in which if the specified path is not detected in step 6 of the certificate validation step, judging that the public key certificate of which certificate validation is requested is not valid, and outputting the result of the judgment (see */S2003 in FIG.11;* and for example, par.[0103] of **Fujishiro**).

Claim 9 is a computer program product claim of the method recited in Claim 2. It is rejected for the same rationale applied to the rejection of the method of Claim 2.

As per Claims 3 and 4, Fujishiro-Van Oorschot combination teaches,

step 11) validating a revocation list issued by the end entity certificate issuing authority as to the public key certificated issued by the end entity certificate issuing authority in step 2 by using the public key certificate issued to the end entity certificate issuing authority (see for example, par.[0057] and [0092] of **Fujishiro**); step 12) if the validation key certificate in step 11 is successful, registering the revocation

list as a valid revocation list in the database, in association with the valid path to be registered in step 3 (see *CERTIFICATION HOLDING UNIT 25 in FIG.*4; for example, par.[0056] and [0092] of **Fujishiro**); step 13) as the public key certificate issued by the end entity certificate issuing authority which is the end of the partial path in step 7, validating the revocation list issued by the end entity certificate issuing authority by using the public key certificate issued to the end entity certificate issuing authority (see for example, par.[0067], [0056] of **Fujishiro**); step 14) if the validation in step 13 is successful, registering the revocation list as a valid revocation list in the database in association with the partial path to be registered in the database in step 9 (see for example, par.[0079] to [0085] of **Fujishiro**); step 15) checking in step 5, whether the public key certificate of which the certificate validation is requested is invalid or not, using the valid revocation list which has been registered in association with the checked path (see *TERM/REVOCATION STATE EXAMINATION UNIT 38 and CRL CREATION SCHEDULE TIME DB in FIG.*5; for example, par.[0057] and [0062] to [0066] of **Fujishiro**); and step 16) if the signature validation in step 5 is successful and the public key certificate of which the validation is requested is valid in step 15, judging that the public key certificate of which certificate validation is requested is valid, and if the signature validation is failed, or the public key certificate of which the validation is requested is invalid, judging that the public key certificate of which certificate validation is requested is not valid (see for example, par.[0057], [0065] and [0093] to [0098] of **Fujishiro**).

Claims 10 and 11 are computer program product claims of the method recited in Claims 3 and 4. They are rejected for the same rationale applied to the rejection of the method of Claims 3 and 4.

As per Claims 5 and 6, Fujishiro-Van Oorschot combination teaches,

step 17) if the path checked in step 4 of the certificate validation step is registered as the valid path in the database, checking in step 5 whether the public key certificate of which the certificate validation is requested or any other public key certificates issued by other certificate authorities included in the checked path includes any constraint item [see for example, par. [0090] of **Fujishiro**); if the path includes any constraint item, checking whether the checked path observes the constraint (see for example, par.[0055] and [0104] of **Fujishiro**); and if the path observes the constraint, judging that the

public key certificate of which the certificate validation is requested is valid (see for example, par.[0105] and [0106] of **Fujishiro**); step 18) if the path checked in the step 4 of the certificate validation step is registered in the database as the valid path, checking in step 5, whether the certificate validation request includes any policy and checking whether the public key certificate of which the certificate validation is requested or other public key certificates issued by any other certificate authorities included in the checked path satisfies the policy included in the certificate validation request (see for example, par.[0055] and [0107] of **Fujishiro**); and if the public key certificate of which the certificate validation is requested or other public key certificates satisfies the policy, judging that the public key certificate of which the certificate validation is requested is valid (see for example, par.[0108] and [0109] of **Fujishiro**).

Claims 12 and 13 are computer program product claims of the method recited in Claims 5 and 6. They are rejected for the same rationale applied to the rejection of the method of Claims 5 and 6.

As per Claim 7, Fujishiro-Van Oorschot combination teaches,

in a case where, at the validity validation step, the path corresponding to the validity validation request is registered as the valid path in the database (see *VALIDITY TERM/REVOCATION STATE EXAMINATION UNIT 34 in FIG.5*; and for example, par.[0065] of **Fujishiro**), it is validated without validating the certificate revocation list that the pertinent public key certificate is not revoked (see *S1008 VERIFY PATH ASSOCIATED WITH TERM_EXPIRED CERTIFICATE, BY USING NEW CERTIICATE in FIG.7;* and for example, par.[0093] to [0098] of **Fujishiro**).

Claim 14 is a computer program product claim of the method recited in Claim 7. It is rejected for the same rationale applied to the rejection of the method of Claim 7.

CONTACT INFORMATION

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2439)
/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2439